2134

PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

JUN 26 2006 PATENT & TRADEMARK OFFICE

(to be used for all correspondence after initial filing)

		Application Number	09/982,260
		Filing Date	10/17/2001
		First Named Inventor	Johan P. Linnartz
		Art Unit	2134
		Examiner Name	Christopher J. Brown
Total Number of Pages in This Submission	33	Attorney Docket Number	NL000558

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [x] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [x] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [ ] Other Enclosure(s) (please Identify below):

Remarks

Enclosed is an Appeal Brief and the requried fee. This brief is being submitted on the first busines day following a Saturday due date, therefore, no extension is required.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	LEIMBACH ASSOCIATES		
Signature	James D. Leimbach		
Printed name	James D. Leimbach		
Date	June 19, 2006	Reg. No.	34,374

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	James D. Leimbach		
Typed or printed name	James D. Leimbach	Date	June19, 2006

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/17 (12-04v2)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

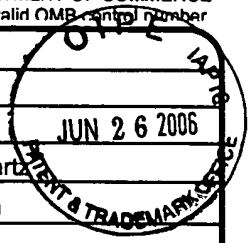
Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL
For FY 2005

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT	($)	500.00

Complete if Known	
Application Number	09/982,260
Filing Date	10/17/2001
First Named Inventor	Johan P. M. G. Linnartz
Examiner Name	Christopher J. Brown
Art Unit	2134
Attorney Docket No.	NL000558



METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☑ Deposit Account Deposit Account Number: 50-3745 Deposit Account Name: _____

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☑ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES Fee ($)	FILING FEES Small Entity Fee ($)	SEARCH FEES Fee ($)	SEARCH FEES Small Entity Fee ($)	EXAMINATION FEES Fee ($)	EXAMINATION FEES Small Entity Fee ($)	Fees Paid ($)
Utility	300	150	500	250	200	100	
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - 20 or HP =	_____	x _____	= _____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - 3 or HP =	_____	x _____	= _____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims Fee ($)	Multiple Dependent Claims Fee Paid ($)
_____	_____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee ($)	Fee Paid ($)
_____ - 100 =	_____ / 50 =	_____ (round up to a whole number)	x _____	= _____

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	
Other (e.g., late filing surcharge): Fee for Appeal Brief	500

SUBMITTED BY

Signature	James D. Leimbach	Registration No. (Attorney/Agent) 34,374	Telephone (585) 381-9983
Name (Print/Type)	James D. Leimbach		Date 06/19/2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of John P. Linnartz MULTIPLE AUTHENTICATION SESSIONS FOR CONTENT PROTECTION Serial No. 09/982,260 Filed: October 17, 2001 Confirmation No. 7206	Group Art Unit: 2134 Examiner: Christopher J. Brown I hereby certify that this correspondence is being deposited today with the United States Postal Services as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patent Commissioner for Patents P.O. Box 1450 Alexandria VA. 22313-1450 Name: James D. Leimbach Registration No. 34,374 Date: June 19, 2006

Mail Stop Appeal Brief-Patent
Honorable Commissioner of Patents and Trademarks
Alexandria VA. 22313-1450

Sir:

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Real party in interest

The real party of interest is the Assignee who is U. S. Philips Corporation, a corporation existing under the laws of the State of Delaware (hereinafter Appellant).

Related appeals and interferences

There are no related appeals or interferences to the present application that are known to appellants, the appellant's legal representative, or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

Status of the Claims

Claims 1-20 are drawn to a method, device and signal for secure data communication to transfer content between consumer devices by: a) activating a data communication link between the devices, b) transmitting data between the devices for performing an authentication session for authenticating the consumer devices, wherein the authentication session generates a first key; c) transmitting data between the devices for performing a subsequent authentication session for authenticating the consumer devices, wherein the subsequent authentication session generates a second key used in transferring audio or visual content. Claims 1-20 stand rejected as the claims that are currently being appealed. A copy of appealed claims 1-20 is contained in Appendix III following this brief.

Status of the Amendments After Final

A response was filed subsequent to the final rejection to overcome the Examiner's rejection of claims 11-22 under 35 U.S.C. §112, second paragraph, and 35 U.S.C. §103(a). The Examiner in an Advisory Action dated March 15, 2006 indicated that the rejections of claims 1-20 under U.S.C. §112, second paragraph, and 35 U.S.C. §103(a) stand.

Summary of the Claimed Subject Matter

The appealed claims define subject matter for a a method, device and signal for secure data communication to transfer content between consumer devices by: a) activating a data communication link between the devices, b) transmitting data between the devices for performing an authentication session for authenticating the consumer devices, wherein the authentication session generates a first key; c) transmitting data between the devices for performing a subsequent authentication session for authenticating the consumer devices, wherein the subsequent authentication session generates a second key used in transferring audio or visual content.

Appealed claim 1 defines subject matter for a method for secure data communication to transfer content between consumer devices as illustrated in Figure 1. The activating of a data communication link between the devices is described in the specification on page 5, lines 1-3. The transmitting of data between the devices for performing an authentication session (3) for authenticating the consumer devices (1, 2) is described in the specification on page 5, line 3- page 6, line 2. The generation of a first key (5) during the authentication session (3) is described in the specification from page 5, line 3-page 6, line 2. The method of appealed claim1 is further characterized in the transmitting data between the devices for performing a subsequent authentication session (4) as described in the specification on page 6, lines 4-7 for authenticating the consumer devices (1, 2), wherein the subsequent authentication session (4) generates a second key (6) as described in the specification on page 6, lines3-21 that is used in transferring audio or visual content as described in the specification from page 7, line 19-page 8, line 10.

Appealed claim 13 defines subject matter for the consumer device as claimed in claim 9, wherein the consumer device (1, 2) comprises means (Bluetooth technology) for performing short-range wireless data communication as described in the specification to the present invention on page 5, lines 1-7.

Grounds of Rejection to be Reviewed on Appeal

The Advisory Action mailed March 15, 2006 indicated that the rejections to claim 1-20 stand. Claims 1 through 20 are the appealed claims. Appealed claim 5 is rejected under the

provisions of 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim subject matter of invention, specifically, appealed claim 5 is rejected being an omnibus type claim for containing a reference to the Bluetooth Specification. Appealed claims 1, 3, 4, 9, 11-15, 17 and 19 are rejected under the provisions of 35 U.S.C. §103(a) has been obvious over U.S. Patent No. 5,915,021 issued in the name of Herlin et al. (hereinafter referred to as *Herlin et al.*) in view U.S. Patent No. 6,487,663 issued in the name of Jaisimha et al. (hereinafter referred to as *Jaisimha et al.*). Appealed claims 2, 5, 6, 7 and 16 are rejected under the provisions of 35 U.S.C. §103(a) has been obvious over *Herlin et al.* in view of *Jaisimha et al.* and further in view of the Bluetooth Specification Version 1.0B. Appealed claim 8 is rejected under the provisions of 35 U.S.C. §103(a) has been obvious over *Herlin et al.* in view of *Jaisimha et al.* and further in view of U.S. Patent No. 5,604,802 issued in the name of Holloway (hereinafter referred to as *Holloway*). Appealed claim 10 is rejected under the provisions of 35 U.S.C. §103(a) has been obvious over *Herlin et al.* in view of *Jaisimha et al.* and further in view of U.S. Patent No. 6,839,437 issued in the name of Crane et al. (hereinafter referred to as *Crane et al.*). Appealed claims 18 and 20 are rejected under the provisions of 35 U.S.C. §103(a) has been obvious over *Herlin et al.* in view of *Jaisimha et al.* and further in view of U.S. Patent No. 6,487,663 issued in the name of Moskowitz (hereinafter referred to as *Moskowitz*).

Argument

I. The rejection of appealed claim 5 under the provisions of 35 U.S.C. §112, second paragraph, as being indefinite for failing to distinctly claim and particularly point out invention

Appealed claim 5

Appealed claim defines subject matter for the method as claimed in claim 1, wherein the first authentication session is an authentication session as described in the BLUETOOTH link encryption specification. The specification to the present invention on page 1, lines 15-18 discusses that the "Specification of the Bluetooth System", v1.0B, December 1st

1999, Specification Volume 1 (Core), Part B Baseband Specification. In this Specification the Bluetooth link encryption is standardized. Therefore, the term Bluetooth link encryption specification is defined by the specification to the present invention.

The specification further details the Bluetooth link encryption specification on page 1, line 18-page2, line 13 by stating that this "link encryption is based on a symmetric cryptographic algorithm. The cryptographic keys as used in this algorithm are derived from a consumer device ID and an authentication process. An authentication process is a process which is used by a consumer device to prove to another consumer device that it is actually the device it tells it is. The authentication process as performed in the Bluetooth link encryption is designed to provide user privacy when the user communicates between two of his two devices. This is achieved in the following way: the user chooses which device(s) he trust and brings `in close contact` his user device and another consumer device. These two devices must share a common cryptographic secret. It is the user's responsibility that no eavesdropper can tap into the exchange of messages and modify the message content. Another authentication session is performed in the Bluetooth link encryption when the user chooses a PIN code in order to ensure that no unauthorized person can use his Bluetooth device(s). The PIN code is used here to authenticate the user.

However, if the system is used to exchange digital content for which the user has to pay, the user may be tempted to try and break the security. By changing the PIN number numerous times, a malicious user might be able to gain information on the security system and eventually be able to retrieve some or all the link keys and the encryption key. This means that the user is able to intercept and decrypt encrypted content or authenticate non-compliant devices.

It is clear that when using the Bluetooth link encryption the user of the devices chooses which device he trusts. This link encryption is therefore not suitable in the situation in which the user is not trusted and can not be asked to play the role of trusted authority. This is, for example, relevant in the case where it must be prohibited that the user can attach to the device and copy or get access to content, stored on this device, illegally."

Therefore, the subject matter for Bluetooth link encryption specification should be interpreted in a manner consistent with the definition supplied by the specification. This definition is a clear definition that is not indefinite and, moreover, particularly points out and distinctly defines the subject matter included by appealed claim 5. In view of the foregoing, the

appellants respectfully submit that appealed claim 5 particularly points out and distinctly claims the subject matter of the invention.

II. The rejection of appealed claims 1, 3, 4, 9, 11-15, 17 and 19 under the provisions of 35 U.S.C. §103(a) as being obvious over *Herlin et al.* in view of *Jaisimha et al.*

A. The rejection under 35 U.S.C. S 103(a)

Appealed claims 1, 3, 4, 9, 11-15, 17 and 19 under the provisions of 35 U.S.C. §103(a) as being obvious over *Herlin et al.* (U.S. Patent No. 5,915,021) in view of *Jaisimha et al.* (U.S. Patent No. 6,487,663). The examiner's position is that it would have been obvious to one of ordinary skill within the art to apply the teaching of *Jaisimha et al.* to *Herlin et al.* to create the subject matter defined by appealed claims 1, 3, 4, 9, 11-15, 17 and 19. The examiner states that *Herlin et al.* discloses all the subject matter of the rejected claims except for using a key to transfer audio or visual content. The examiner's position is that *Jaisimha et al.* teach that a media player that exchanges audio and visual content.

The MPEP at §2142 regarding the concept of *Prima Facie* Obviousness that the examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness.

The MPEP at §2143 states regarding the basic requirements of a *Prima Facie* case of obviousness, to "establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure." *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

The MPEP at §2143.01 states that if "proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no

suggestion or motivation to make the proposed modification. *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984).

The MPEP at §2143.01 states that if "the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)".

B. The references

Herlin et al. (U.S. Patent No. 5,915,021) teach a method for secure communications in a telecommunication system (see Title). The teaching of *Herlin et al.* relate to sending a secure message in a telecommunications system utilizing public encryption keys. The authentication parameters, including decryption keys, are known only to a user and used to verify the identity of a sender of a communication to another user by public key methods. *Herlin et al.* teach that once the initialization is completed the a private encryption key can be generated and used for encryption. *Herlin et al.* teach that two keys can be generated. A first key for authentication and a second encryption key used both in authentication and for encrypting subsequent communications (see Abstract).

Herlin et al. teach that two session keys are generated. A first session is used only in the authentication process. A second session key is used in both in the authentication process and for the encrypting of subsequent communications (sees col. 5, lines 1-9). It should be noted that the first session key and the second session key are selected by the mobile station and the base station within *Herlin et al.* (see col. 5, lines 35-47). There is no generation of these keys that occurs during either a first or second authentication process.

There is no disclosure or suggestion within *Herlin et al.* for a subsequent authentication, wherein the subsequent authentication session generates a second key. There is further no disclosure or suggestion for a subsequent authentication session for authenticating the consumer devices, wherein the subsequent authentication session generates a second key used in transferring audio or visual content.

Jaisimha et al. teach a system and method for regulating the transmission of data (see Title). *Jaisimha et al.* relate to the transmission of media data, wherein a header portion

within the media file is encoded to include an access code (see Abstract). It is fully intended by *Jaisimha et al.* that the access code within the header portion of the media file be used to determine if the media file can be transmitted (see col. 2, line 15-col. 4, line 10).

While, *Jaisimha et al.* teach that a media player that exchanges audio and visual content at col. 4, lines 36-42, it would be contrary to the principle of operation for method and system taught therein for access to the media file to be gained by other means than an access code within the header portion. Furthermore, *Jaisimha et al.* there is no disclosure or suggestion within *Jaisimha et al.* that *Jaisimha et al.* could operate with a reasonable expectation of success using keys and authentication processes. *Jaisimha et al.* do not disclose or suggest generation of keys during authentication sessions.

C. The differences between the invention and the references

Appealed claim 1

Appealed claim 1 defines subject matter for a method for secure data communication to transfer content between consumer devices, including: activating a data communication link between the devices; transmitting data between the devices for performing an authentication session for authenticating the consumer devices, wherein the authentication session generates a first key; and transmitting data between the devices for performing a subsequent authentication session for authenticating the consumer devices, wherein the subsequent authentication session generates a second key used in transferring audio or visual content. There is no disclosure or suggestion within *Herlin et al.* or *Jaisimha et al.*, either alone or in combination, for a method for secure data communication to transfer content between consumer devices, including: activating a data communication link between the devices; transmitting data between the devices for performing an authentication session for authenticating the consumer devices, wherein the authentication session generates a first key; and transmitting data between the devices for performing a subsequent authentication session for authenticating the consumer devices, wherein the subsequent authentication session generates a second key used in transferring audio or visual content.

Appealed claim 3

Appealed claim 3 defines subject matter for the method defined by appealed claim 1, characterized in that the authentication sessions are performed independent of each other. There is no disclosure or suggestion within *Herlin et al.* or *Jaisimha et al.*, either alone or in combination, for the method as defined by appealed claim 1, characterized in that the authentication sessions are performed independent of each other.

Appealed claim 4

Appealed claim 4 defines the subject matter defined by claim 1, characterized in that transmitting data between the devices for performing an authentication session further includes transmitting additional data between the devices for deciding whether of not to proceed with transmitting data between the devices for performing a subsequent authentication session. There is no disclosure or suggestion within *Herlin et al.* or *Jaisimha et al.*, either alone or in combination, for the method as defined by appealed claim 1, characterized in that transmitting data between the devices for performing an authentication session further includes transmitting additional data between the devices for deciding whether of not to proceed with transmitting data between the devices for performing a subsequent authentication session.

Appealed claim 9

Appealed claim 9 defines subject matter for a consumer device for performing the method according to claim 1, the consumer device comprising means for activating a data communication link, means for transmitting data, authentication means for performing an authentication session and further authentication means for performing another authentication session. There is no disclosure or suggestion within *Herlin et al.* or *Jaisimha et al.*, either alone or in combination, for a consumer device for performing the method according to claim 1, the consumer device comprising means for activating a data communication link, means for transmitting data, authentication means for performing an authentication session and further authentication means for performing another authentication session.

Appealed claim 11

Appealed claim 11 defines subject matter for the consumer device defined by claim 9, characterized in that the consumer device further comprises receiving means for receiving information, decrypting means for decrypting the information using the link key and recording means for recording the information. There is no disclosure or suggestion within *Herlin et al.* or *Jaisimha et al.*, either alone or in combination, for the consumer device defined by claim 9, characterized in that the consumer device further comprises receiving means for receiving information, decrypting means for decrypting the information using the link key and recording means for recording the information.

Appealed claim 12

Appealed claim 12 defines the consumer device as claimed in claim 9, wherein the consumer device is a portable device, e.g. a headphone or a walkman. There is no disclosure or suggestion within *Herlin et al.* or *Jaisimha et al.*, either alone or in combination, for the consumer device defined by claim 9, wherein the consumer device is a portable device, such as a headphone or a walkman.

Appealed claim 13

Appealed claim 13 defines subject matter for the consumer device as claimed in claim 9, wherein the consumer device comprises means for performing short-range wireless data communication. There is no disclosure or suggestion within *Herlin et al.* or *Jaisimha et al.*, either alone or in combination, for the consumer device defined by claim 9, wherein the consumer device comprises means for performing short-range wireless data communication.

Appealed claim 14

Appealed claim 14 defines subject matter for a signal comprising data transmitted between the devices as used in claim 1, wherein the data is used for performing the authentication sessions for authenticating the devices. There is no disclosure or suggestion within *Herlin et al.* or *Jaisimha et al.*, either alone or in combination, for the subject matter for a signal comprising data transmitted between the devices as used in claim 1, wherein the data is used for performing the authentication sessions for authenticating the devices.

Appealed claim 15

Appealed claim 15 defines subject matter for a signal comprising a first key and a second key obtained after performing the method of claim 1. There is no disclosure or suggestion within *Herlin et al.* or *Jaisimha et al.*, either alone or in combination, for a signal comprising a first key and a second key obtained after performing the method of claim 1.

Appealed claim 17

Appealed claim 17 defines the subject matter for the method of claim 1wherein transferring audio or visual content further comprises before transferring, determining a compliance level. There is no disclosure or suggestion within *Herlin et al.* or *Jaisimha et al.*, either alone or in combination, for the subject matter for the method of claim 1wherein transferring audio or visual content further comprises before transferring, determining a compliance level.

Appealed claim 19

Appealed claims 19 defines the subject matter for the method of claim 1 wherein during the subsequent authentication session a device for downloading audio or visual content proves that it is allowed to download the content. There is no disclosure or suggestion within *Herlin et al.* or *Jaisimha et al.*, either alone or in combination, for the method of claim 1 wherein during the subsequent authentication session a device for downloading audio or visual content proves that it is allowed to download the content.

Appealed claim 20

Appealed claim 20 defines subject matter for the method of claim 19 wherein during the subsequent authentication session the device for downloading audio or visual content is limited in terms of quality for content it is allowed to download in response to a result from the subsequent authentication session. There is no disclosure or suggestion within *Herlin et al.* or *Jaisimha et al.*, either alone or in combination, for the method of claim 19 wherein during the subsequent authentication session the device for downloading audio or visual content is limited

in terms of quality for content it is allowed to download in response to a result from the subsequent authentication session.

III. The rejection of appealed claims 2, 5, 6, 7 and 16 under the provisions of 35 U.S.C. §103(a) as being obvious over *Herlin et al.* in view of *Jaisimha et al.* and further in view of Bluetooth Security Specfication

A. The rejection under 35 U.S.C. S 103(a)

Appealed claims 2, 5, 6, 7 and 16 are rejected under the provisions of 35 U.S.C. §103(a) as being obvious over *Herlin et al.* (U.S. Patent No. 5,915,021) in view of *Jaisimha et al.* (U.S. Patent No. 6,487,663) and further in view of Bluetooth Security Specfication Version 1.0B. The examiner's position is that the combination of *Herlin et al.* with *Jaisimha et al.* teaches the generation of a first key and a second but not merging.

The MPEP at §2142 regarding the concept of *Prima Facie* Obviousness that the examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness.

The MPEP at §2143 states regarding the basic requirements of a *Prima Facie* case of obviousness, to "establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure." *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

The MPEP at §2143.01 states that if "proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984).

The MPEP at §2143.01 states that if "the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)".

B. The references

Herlin et al. (U.S. Patent No. 5,915,021) teach a method for secure communications in a telecommunication system (see Title). The teaching of *Herlin et al.* relate to sending a secure message in a telecommunications system utilizing public encryption keys. The authentication parameters, including decryption keys, are known only to a user and used to verify the identity of a sender of a communication to another user by public key methods. *Herlin et al.* teach that once the initialization is completed the a private encryption key can be generated and used for encryption. *Herlin et al.* teach that two keys can be generated. A first key for authentication and a second encryption key used both in authentication and for encrypting subsequent communications (see Abstract).

Herlin et al. teach that two session keys are generated. A first session is used only in the authentication process. A second session key is used in both in the authentication process and for the encrypting of subsequent communications (sees col. 5, lines 1-9). It should be noted that the first session key and the second session key are selected by the mobile station and the base station within *Herlin et al.* (see col. 5, lines 35-47). There is no generation of these keys that occurs during either a first or second authentication process.

There is no disclosure or suggestion within *Herlin et al.* for a subsequent authentication, wherein the subsequent authentication session generates a second key. There is further no disclosure or suggestion for a subsequent authentication session for authenticating the consumer devices, wherein the subsequent authentication session generates a second key used in transferring audio or visual content.

Jaisimha et al. teach a system and method for regulating the transmission of data (see Title). *Jaisimha et al.* relate to the transmission of media data, wherein a header portion within the media file is encoded to include an access code (see Abstract). It is fully intended by *Jaisimha et al.* that the access code within the header portion of the media file be used to determine if the media file can be transmitted (see col. 2, line 15-col. 4, line 10).

While, *Jaisimha et al.* teach that a media player that exchanges audio and visual content at col. 4, lines 36-42, it would be contrary to the principle of operation for method and system taught therein for access to the media file to be gained by other means than an access code within the header portion. Furthermore, *Jaisimha et al.* there is no disclosure or suggestion within *Jaisimha et al.* that *Jaisimha et al.* could operate with a reasonable expectation of success using keys and authentication processes. *Jaisimha et al.* do not disclose or suggest generation of keys during authentication sessions.

The Bluetooth Security specification Version 1.0B teaches generation of a combination key beginning on page 155. The Bluetooth Security specification Version 1.0B clearly teaches that the combination key is generated during the initialization procedure (see first paragraph of section 14.2.2.4). The Bluetooth Security specification Version 1.0B teaches on the top of page 156 that a 128-bit link key is generated during initialization by a bitwise modulo-2 addition (XOR). The appellant, respectfully, points out that the Bluetooth Security specification Version 1.0B clearly teaches that an authentication process is initiated after generation of the combination key. There is no disclosure or suggestion for generating a key during an authentication process by the Bluetooth Security specification Version 1.0B.

C. The differences between the invention and the references

The appellant respectfully refers the Board to the arguments made under the response to the rejection of appealed claims 1, 3, 4, 9, 11-15, 17 and 19 under the provisions of 35 U.S.C. §103(a) as being obvious over *Herlin et al.* in view of *Jaisimha et al.*

The rejection asserts that the combination of *Herlin et al.* with *Jaisimha et al.* teaches generation of keys. As previously discussed under the response to the rejection of appealed claims 1, 3, 4, 9, 11-15, 17 and 19 under the provisions of 35 U.S.C. §103(a) as being obvious over *Herlin et al.* in view of *Jaisimha et al.*, the combination of *Herlin et al.* with *Jaisimha et al.* do not disclose or suggest the generation of keys during authentication processes as defined by the appealed claims.

The rejection asserts that the Bluetooth Security specification Version 1.0B teaches merging to form keys. The appellant, respectfully, points out that the Bluetooth Security specification Version 1.0B does not disclose or suggest the generation of keys during authentication processes as defined by the appealed claims.

Appealed claim 2

Appealed claim 2 defines subject matter for the method defined by appealed claim 1, further including generating a link key for encrypting and/or decrypting the data communicated over the data communication link by merging the first key with the second key using a key merge function. There is no disclosure or suggestion within *Herlin et al.*, *Jaisimha et al.* or the Bluetooth Security specification Version 1.0B, either alone or in combination, for the method of claim 1 further including generating a link key for encrypting and/or decrypting the data communicated over the data communication link by merging the first key with the second key using a key merge function.

Appealed claim 5

Appealed claim 5 defines subject matter for the method defined by appealed claim 1, further including the first authentication session is an authentication session as described in the BLUETOOTH link encryption specification. There is no disclosure or suggestion within *Herlin et al.*, *Jaisimha et al.* or the Bluetooth Security specification Version 1.0B, either alone or in combination, for the method of claim 1 further including the first authentication session is an authentication session as described in the BLUETOOTH link encryption specification.

Appealed claim 6

Appealed claim 6 defines subject matter for the method defined by appealed claim 2, further characterized in that the key merge function has one or more of the following properties: for any two given first and second keys as input in the key merge function, the link key output of the key merge function is uniquely specified; the number of link key output bits is constant;--if the second key is undefined or all zero, the link key output bits are identical to the bits of the first key; for any first key, the uncertainty in the output is approximately equal to the uncertainty of the second key; for any second key, the uncertainty in the output is approximately equal to the uncertainty of the first key. There is no disclosure or suggestion within *Herlin et al.*, *Jaisimha et al.* or the Bluetooth Security specification Version 1.0B, either alone or in

combination, for the method of claim 2, further characterized in that the key merge function has one or more of the following properties: for any two given first and second keys as input in the key merge function, the link key output of the key merge function is uniquely specified; the number of link key output bits is constant;--if the second key is undefined or all zero, the link key output bits are identical to the bits of the first key; for any first key, the uncertainty in the output is approximately equal to the uncertainty of the second key; for any second key, the uncertainty in the output is approximately equal to the uncertainty of the first key.

Appealed claim 7

Appealed claim 7 defines subject matter for the method defined by appealed claim 6, characterized in that the key merge function is a bit-wise XOR-function. There is no disclosure or suggestion within *Herlin et al.*, *Jaisimha et al.* or the Bluetooth Security specification Version 1.0B, either alone or in combination, for the method of claim 6, characterized in that the key merge function is a bit-wise XOR-function.

Appealed claim 16

Appealed claim 16 defines subject matter for the method defined by appealed claim 15, characterized in that it further comprises a link key for encrypting and/or decrypting audio or video content data communicated over the data communication link, the link key being generated by merging the first key with the second key using a key merge function. There is no disclosure or suggestion within *Herlin et al.*, *Jaisimha et al.* or the Bluetooth Security specification Version 1.0B, either alone or in combination, for the method of claim15, characterized in that it further comprises a link key for encrypting and/or decrypting audio or video content data communicated over the data communication link, the link key being generated by merging the first key with the second key using a key merge function.

IV. The rejection of appealed claim 8 under the provisions of 35 U.S.C. §103(a) as being obvious over *Herlin et al.* in view of *Jaisimha et al.* and further in view of U.S. Patent No. 5,604,802 issued to Holloway (hereinafter referred to as *Holloway*)

A. The rejection under 35 U.S.C. S 103(a)

Appealed claim 8 is rejected under the provisions of 35 U.S.C. §103(a) as being obvious over *Herlin et al.* in view of *Jaisimha et al.* and further in view of *Holloway* (U.S. Patent No. 5,604,802). The examiner's position is that it would have been obvious to one of ordinary skill within the art to apply the teaching of *Jaisimha et al.* to *Herlin et al.* to create the subject matter defined by appealed claims 1, 3, 4, 9, 11-15, 17 and 19. The examiner states that *Herlin et al.* discloses all the subject matter of the rejected claims except for using a key to transfer audio or visual content. The examiner's position is that *Jaisimha et al.* teach that a media player that exchanges audio and visual content.

The MPEP at §2142 regarding the concept of *Prima Facie* Obviousness that the examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness.

The MPEP at §2143 states regarding the basic requirements of a *Prima Facie* case of obviousness, to "establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure." *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

The MPEP at §2143.01 states that if "proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984).

The MPEP at §2143.01 states that if "the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)".

B. The references

Herlin et al. (U.S. Patent No. 5,915,021) teach a method for secure communications in a telecommunication system (see Title). The teaching of *Herlin et al.* relate to sending a secure message in a telecommunications system utilizing public encryption keys. The authentication parameters, including decryption keys, are known only to a user and used to verify the identity of a sender of a communication to another user by public key methods. *Herlin et al.* teach that once the initialization is completed the a private encryption key can be generated and used for encryption. *Herlin et al.* teach that two keys can be generated. A first key for authentication and a second encryption key used both in authentication and for encrypting subsequent communications (see Abstract).

Herlin et al. teach that two session keys are generated. A first session is used only in the authentication process. A second session key is used in both in the authentication process and for the encrypting of subsequent communications (sees col. 5, lines 1-9). It should be noted that the first session key and the second session key are selected by the mobile station and the base station within *Herlin et al.* (see col. 5, lines 35-47). There is no generation of these keys that occurs during either a first or second authentication process.

There is no disclosure or suggestion within *Herlin et al.* for a subsequent authentication, wherein the subsequent authentication session generates a second key. There is further no disclosure or suggestion for a subsequent authentication session for authenticating the consumer devices, wherein the subsequent authentication session generates a second key used in transferring audio or visual content.

Jaisimha et al. teach a system and method for regulating the transmission of data (see Title). *Jaisimha et al.* relate to the transmission of media data, wherein a header portion within the media file is encoded to include an access code (see Abstract). It is fully intended by *Jaisimha et al.* that the access code within the header portion of the media file be used to determine if the media file can be transmitted (see col. 2, line 15-col. 4, line 10).

While, *Jaisimha et al.* teach that a media player that exchanges audio and visual content at col. 4, lines 36-42, it would be contrary to the principle of operation for method and system taught therein for access to the media file to be gained by other means than an access code within the header portion. Furthermore, *Jaisimha et al.* there is no disclosure or suggestion

within *Jaisimha et al.* that *Jaisimha et al.* could operate with a reasonable expectation of success using keys and authentication processes. *Jaisimha et al.* do not disclose or suggest generation of keys during authentication sessions.

Holloway (U.S. Patent No. 5,604,802) relates to a transaction processing system (see Title) and generating a transaction message that has a transaction terminal that receives characteristic data from a user that generates an image associated with the user (see Abstract). *Holloway* on col. 9, lines 45-53 teach that encryption keys retransferred between cryptographic units are enciphered using higher level keys and that the higher level keys are enciphered using a portion of the transferred key. It should be noted that there is no disclosure or suggestion for generation of keys during an authentication session by *Holloway*.

C. The differences between the invention and the references

The appellant respectfully refers the Board to the arguments made under the response to the rejection of appealed claims 1, 3, 4, 9, 11-15, 17 and 19 under the provisions of 35 U.S.C. §103(a) as being obvious over *Herlin et al.* in view of *Jaisimha et al.*

Appealed claim 8

Appealed claim 8 defines subject matter for the method defined by appealed claim 2, characterized in that the key merge function comprises encrypting the first key with the second key or vice versa. There is no disclosure or suggestion within *Herlin et al.*, *Jaisimha et al.* or *Holloway*, either alone or in combination, for the method of claim2, characterized in that the key merge function comprises encrypting the first key with the second key or vice versa.

V. The rejection of appealed claim 10 under the provisions of 35 U.S.C. §103(a) as being obvious over *Herlin et al.* in view of *Jaisimha et al.* and further in view of U.S. Patent No. 6,839,437 issued to Crane et al. (hereinafter referred to as *Crane et al.*)

A. The rejection under 35 U.S.C. S 103(a)

Appealed claim 10 is rejected under the provisions of 35 U.S.C. §103(a) as being obvious over *Herlin et al.* in view of *Jaisimha et al.* and further in view of *Crane et al.*. (U.S.

Patent No. 6,839,437). The examiner's position is that the combination of *Jaisimha et al.* with *Herlin et al.* does not teach the use of an Application Programmers Interface (API). The examiner states that *Crane et al.* teach the use of an API.

The MPEP at §2142 regarding the concept of *Prima Facie* Obviousness that the examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness.

The MPEP at §2143 states regarding the basic requirements of a *Prima Facie* case of obviousness, to "establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure." *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

The MPEP at §2143.01 states that if "proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984).

The MPEP at §2143.01 states that if "the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)".

B. The references

Herlin et al. (U.S. Patent No. 5,915,021) teach a method for secure communications in a telecommunication system (see Title). The teaching of *Herlin et al.* relate to sending a secure message in a telecommunications system utilizing public encryption keys. The authentication parameters, including decryption keys, are known only to a user and used to

verify the identity of a sender of a communication to another user by public key methods. *Herlin et al.* teach that once the initialization is completed the a private encryption key can be generated and used for encryption. *Herlin et al.* teach that two keys can be generated. A first key for authentication and a second encryption key used both in authentication and for encrypting subsequent communications (see Abstract).

Herlin et al. teach that two session keys are generated. A first session is used only in the authentication process. A second session key is used in both in the authentication process and for the encrypting of subsequent communications (sees col. 5, lines 1-9). It should be noted that the first session key and the second session key are selected by the mobile station and the base station within *Herlin et al.* (see col. 5, lines 35-47). There is no generation of these keys that occurs during either a first or second authentication process.

There is no disclosure or suggestion within *Herlin et al.* for a subsequent authentication, wherein the subsequent authentication session generates a second key. There is further no disclosure or suggestion for a subsequent authentication session for authenticating the consumer devices, wherein the subsequent authentication session generates a second key used in transferring audio or visual content.

Jaisimha et al. teach a system and method for regulating the transmission of data (see Title). *Jaisimha et al.* relate to the transmission of media data, wherein a header portion within the media file is encoded to include an access code (see Abstract). It is fully intended by *Jaisimha et al.* that the access code within the header portion of the media file be used to determine if the media file can be transmitted (see col. 2, line 15-col. 4, line 10).

While, *Jaisimha et al.* teach that a media player that exchanges audio and visual content at col. 4, lines 36-42, it would be contrary to the principle of operation for method and system taught therein for access to the media file to be gained by other means than an access code within the header portion. Furthermore, *Jaisimha et al.* there is no disclosure or suggestion within *Jaisimha et al.* that *Jaisimha et al.* could operate with a reasonable expectation of success using keys and authentication processes. *Jaisimha et al.* do not disclose or suggest generation of keys during authentication sessions.

Crane et al. (U.S. Patent No. 6,839,437) relates to a method and apparatus for managing keys for cryptographic operations (see Title) and a cryptographic system for use in a data processing system that includes a security layer and a plurality of cryptographic routines,

including a keystore application program interface layer coupled to the security layer (see Abstract). *Crane et al.* on col. 4, lines 13-37 teach that APIs can be used to call various keystrock functions. It should be noted that there is no disclosure or suggestion for a consumer device having an Application Programmers Interface for informing the consumer device about the protection status of another consumer device within *Crane et al.*

C. The differences between the invention and the references

The appellant respectfully refers the Board to the arguments made under the response to the rejection of appealed claims 1, 3, 4, 9, 11-15, 17 and 19 under the provisions of 35 U.S.C. §103(a) as being obvious over *Herlin et al.* in view of *Jaisimha et al.*

Appealed claim 10

Appealed claim 10 defines subject matter for the consumer device defined by claim 9, characterized in that the consumer device further comprises an Application Programmers Interface (API) for informing the consumer device about the protection status of another consumer device. There is no disclosure or suggestion within *Herlin et al.*, *Jaisimha et al.* or *Crane et al.*, either alone or in combination, for the consumer device defined by claim 9, characterized in that the consumer device further comprises an Application Programmers Interface (API) for informing the consumer device about the protection status of another consumer device.

VI. The rejection of appealed claims 18 and 20 under the provisions of 35 U.S.C. §103(a) as being obvious over *Herlin et al.* in view of *Jaisimha et al.* and further in view of U.S. Patent No. 6,598,162 issued to Moskowitz (hereinafter referred to as *Moskowitz*)

A. The rejection under 35 U.S.C. S 103(a)

Appealed claims 18 and 20 are rejected under the provisions of 35 U.S.C. §103(a) as being obvious over *Herlin et al.* in view of *Jaisimha et al.* and further in view of *Moskowitz* (U.S. Patent No. 6,598,162). The examiner's position is that the combination of *Jaisimha et al.* with *Herlin et al.* does not teach the limiting the quality of media. The examiner states that *Moskowitz* teaches the limiting the quality of media.

The MPEP at §2142 regarding the concept of *Prima Facie* Obviousness that the examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness.

The MPEP at §2143 states regarding the basic requirements of a *Prima Facie* case of obviousness, to "establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure." *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

The MPEP at §2143.01 states that if "proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984).

The MPEP at §2143.01 states that if "the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)".

B. The references

Herlin et al. (U.S. Patent No. 5,915,021) teach a method for secure communications in a telecommunication system (see Title). The teaching of *Herlin et al.* relate to sending a secure message in a telecommunications system utilizing public encryption keys. The authentication parameters, including decryption keys, are known only to a user and used to verify the identity of a sender of a communication to another user by public key methods. *Herlin et al.* teach that once the initialization is completed the a private encryption key can be generated and used for encryption. *Herlin et al.* teach that two keys can be generated. A first key for

authentication and a second encryption key used both in authentication and for encrypting subsequent communications (see Abstract).

Herlin et al. teach that two session keys are generated. A first session is used only in the authentication process. A second session key is used in both in the authentication process and for the encrypting of subsequent communications (sees col. 5, lines 1-9). It should be noted that the first session key and the second session key are selected by the mobile station and the base station within *Herlin et al.* (see col. 5, lines 35-47). There is no generation of these keys that occurs during either a first or second authentication process.

There is no disclosure or suggestion within *Herlin et al.* for a subsequent authentication, wherein the subsequent authentication session generates a second key. There is further no disclosure or suggestion for a subsequent authentication session for authenticating the consumer devices, wherein the subsequent authentication session generates a second key used in transferring audio or visual content.

Jaisimha et al. teach a system and method for regulating the transmission of data (see Title). *Jaisimha et al.* relate to the transmission of media data, wherein a header portion within the media file is encoded to include an access code (see Abstract). It is fully intended by *Jaisimha et al.* that the access code within the header portion of the media file be used to determine if the media file can be transmitted (see col. 2, line 15-col. 4, line 10).

While, *Jaisimha et al.* teach that a media player that exchanges audio and visual content at col. 4, lines 36-42, it would be contrary to the principle of operation for method and system taught therein for access to the media file to be gained by other means than an access code within the header portion. Furthermore, *Jaisimha et al.* there is no disclosure or suggestion within *Jaisimha et al.* that *Jaisimha et al.* could operate with a reasonable expectation of success using keys and authentication processes. *Jaisimha et al.* do not disclose or suggest generation of keys during authentication sessions.

Moskowitz (U.S. Patent No. 6,598,162) relates to a method for combining transfer functions with key creation (see Title) wherein the key is a transfer function is a mask to manipulate the granularity of the file for digital samples (see Abstract). *Moskowitz* on col. 4, lines 30-50 teach that when digital information is distributed in encoded form, it may be desirable to allow information to be played at a reduced quality. It should be noted that there is

no disclosure or suggestion within *Moskowitz* for determining compliance levels by users attempting to access data.

C. The differences between the invention and the references

The appellant respectfully refers the Board to the arguments made under the response to the rejection of appealed claims 1, 3, 4, 9, 11-15, 17 and 19 under the provisions of 35 U.S.C. §103(a) as being obvious over *Herlin et al.* in view of *Jaisimha et al.*
The Applicant, respectfully, asserts that none of the foregoing references disclose or suggest a subsequent authentication session for authenticating the consumer devices, wherein the subsequent authentication session generates a second key used in transferring audio or visual content.

There is no disclosure or suggestion within *Moskowitz* for determining compliance levels by users attempting to access data.

Appealed claim 18

Appealed claim 18 defines subject matter for the method of claim 17 wherein determining a compliance level further comprises determining rights that have been placed on content to determine the compliance level. There is no disclosure or suggestion within *Herlin et al.*, *Jaisimha et al.* or *Moskowitz*, either alone or in combination, for the method of claim 17 wherein determining a compliance level further comprises determining rights that have been placed on content to determine the compliance level.

Appealed claim 20

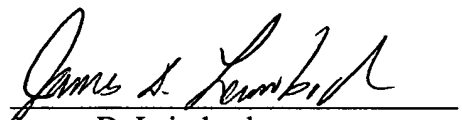
Appealed claims 20 defines subject matter for the method of claim 19 wherein during the subsequent authentication session the device for downloading audio or visual content is limited in terms of quality for content it is allowed to download in response to a result from the subsequent authentication session. There is no disclosure or suggestion within *Herlin et al.*, *Jaisimha et al.* or *Moskowitz*, either alone or in combination, for the method of claim 19 wherein during the subsequent authentication session the device for downloading audio or visual content is limited in terms of quality for content it is allowed to download in response to a result from the subsequent authentication session.

Conclusion

In summary, the examiner's rejections of the claims are believed to be in error for the reasons explained above. The rejections of each of claims 1-20 should be reversed.

The Commissioner is authorized to charge fees associated with the filing of this brief to Account No. 50-3745 including any underpayments, excluding the payment of any issue fees, and to credit any overpayments to the same account.

Respectfully submitted,



James D. Leimbach
Attorney for Appellants
Registration No. 34,374

Telephone: 585-381-9983
Facsimile: 585-381-9983

APPENDIX I. Evidence on Appeal

"None"

APPENDIX II. Related Proceedings

"None"

APPENDIX III. Claims on Appeal

1. Method for secure data communication to transfer content between consumer devices, the method comprising the following steps: a) activating a data communication link between the devices, b) transmitting data between the devices for performing an authentication session for authenticating the consumer devices, wherein the authentication session generates a first key, characterized in that the method further comprises the step of: c) transmitting data between the devices for performing a subsequent authentication session for authenticating the consumer devices, wherein the subsequent authentication session generates a second key used in transferring audio or visual content.

2. The method as claimed in claim 1, characterized in that the method further comprises the step of: d) generating a link key for encrypting and/or decrypting the data communicated over the data communication link by merging the first key with the second key using a key merge function.

3. The method as claimed in claim 1, characterized in that the authentication sessions are performed independent of each other.

4. The method as claimed in claim 1, characterized in that step b) further comprises transmitting additional data between the devices for deciding whether of not to proceed with step c).

5. The method as claimed in claim 1, characterized in that the first authentication session is an authentication session as described in the BLUETOOTH link encryption specification.

6. The method as claimed in claim 2, characterized in that the key merge function has one or more of the following properties: for any two given first and second keys as input in the key merge function, the link key output of the key merge function is uniquely specified; the number of link key output bits is constant;--if the second key is undefined or all zero, the link key output bits are identical to the bits of the first key; for any first key, the uncertainty in the output is approximately equal to the uncertainty of the second key; for any second key, the uncertainty in the output is approximately equal to the uncertainty of the first key.

7. The method as claimed in claim 6, characterized in that the key merge function is a bit-wise XOR-function.

8. The method as claimed in claim 2, characterized in that the key merge function comprises encrypting the first key with the second key or vice versa.

9. Consumer device for performing the method according to claim 1, the consumer device comprising means for activating a data communication link, means for transmitting data, authentication means for performing an authentication session and further authentication means for performing another authentication session.

10. The consumer device as claimed in claim 9, characterized in that the consumer device further comprises an Application Programmers Interface (API) for informing the consumer device about the protection status of another consumer device.

11. The consumer device as claimed in claim 9, characterized in that the consumer device further comprises receiving means for receiving information, decrypting means for decrypting the information using the link key (9) and recording means for recording the information.

12. The consumer device as claimed in claim 9, wherein the consumer device is a portable device, e.g. a headphone or a walkman.

13. The consumer device as claimed in claim 9, wherein the consumer device comprises means for performing short-range wireless data communication.

14. Signal comprising data transmitted between the devices ~~(1,2)~~ as used in claim 1, wherein the data is used for performing the authentication sessions ~~(3,4)~~ for authenticating the devices.

15. Signal comprising a first key and a second key obtained after performing the method of claim 1.

16. Signal according to claim 15, characterized in that it further comprises a link key for encrypting and/or decrypting audio or video content data communicated over the data communication link, the link key being generated by merging the first key with the second key using a key merge function.

17. The method of claim 1wherein transferring audio or visual content further comprises before transferring, determining a compliance level.

18. The method of claim 17 wherein determining a compliance level further comprises determining rights that have been placed on content to determine the compliance level.

19. The method of claim 1 wherein during the subsequent authentication session a device for downloading audio or visual content proves that it is allowed to download the content.

20. The method of claim 19 wherein during the subsequent authentication session the device for downloading audio or visual content is limited in terms of quality for content it is allowed to download in response to a result from the subsequent authentication session.